

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

In the Matter of the Search of

A 2TB Hitachi Hard Drive Serial
Number YFGNBBTA and Labeled
HD-2

Case No. 1:18mj307

APPLICATION FOR AN ORDER TO REQUIRE DEFENDANT BURNS TO
ASSIST IN THE EXECUTION OF A SEARCH WARRANT PURSUANT TO
THE ALL WRITS ACT

NOW COMES the United States of America, by and through Matthew G.T. Martin, United States Attorney for the Middle District of North Carolina, and hereby requests that the Court issue an order compelling Timothy Donovan Burns to produce his 2TB Hitachi hard drive, which is currently in the custody of Homeland Security Investigations (HSI), in an unlocked and decrypted state.

INTRODUCTION

In early 2018, law enforcement identified Timothy Donovan Burns as an individual who was likely downloading child pornography via the Freenet peer-to-peer network. On March 14, 2018, law enforcement agents conducted a knock-and-talk at Burns's residence. Burns made several incriminating statements and consented to the seizure and forensic review of his computer. The review revealed that one of the computer's hard drives, a 2TB Hitachi with

serial number YFGNBBTA, was encrypted. On March 20, 2018, law enforcement agents reengaged Burns at his residence and asked him for the password to the hard drive. Burns unequivocally stated that the hard drive contained child pornography, but declined to provide the password. On October 4, 2018, this Court issued a warrant to search the hard drive. Case No. 1:18mj307. Thereafter, HSI attempted to break the encryption in order to access and search the hard drive. To date, HSI's efforts have been unsuccessful.

On December 17, 2018, a grand jury in the Middle District of North Carolina issued an indictment charging Burns with violations of Title 18 U.S.C. Code §§ 2252A(a)(2)(A), receipt of child pornography, and 2252A(a)(5)(B), possession of child pornography. Case No. 1:18cr492.

By way of this Application the United States seeks an order under the All Writs Act, Title 28 U.S.C. § 1651, requiring Burns to assist in the execution of the previously issued search warrant by producing his 2TB Hitachi hard drive in a fully unencrypted and unlocked state. This can be accomplished by ordering Burns to enter the password without revealing it to law enforcement. The requested relief would not violate Burns's Fifth Amendment privilege against self-incrimination. The contents of the hard drive are not privileged. Further, Burns's act of production would not be testimonial because the only potentially testimonial components implicit in his act of producing the unlocked/unencrypted hard drive are foregone conclusions.

FACTUAL & PROCEDURAL SUMMARY

Identification of Burns as a Suspect:

In January 2018, North Carolina State Bureau of Investigation (SBI) Criminal Specialist (CS) Rodney White observed that an individual with an identified IP address was likely downloading child pornography via the Freenet peer-to-peer network.¹ Internet service provider records revealed that the IP address resolved to “Don Burns” at his apartment located in Kernersville, North Carolina.

Seizure of Electronics & First Interview of Burns:

On March 14, 2018, CS White and HSI SA Charles Cook went to Burns’s apartment to speak with him. Burns answered the door and agreed to speak with the agents inside. Upon entry, the agents observed a desktop computer in the living room connected to a bay of hard drives. Burns explained that he lived alone and was unemployed, though he formerly worked as a computer programmer.

¹ Freenet is an Internet-based, peer-to-peer network that allows users to anonymously share files, chat on message boards, and access websites within the network. When a user uploads a file into Freenet, the software breaks the file into pieces (called “blocks”) and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the Freenet network of users. The software also creates an index piece that contains a list of all of the pieces of the file and a unique key. This key is necessary to download the file.

When asked if he was familiar with file sharing programs, Burns said that he was. He explained that he used the BitTorrent peer-to-peer network² years ago but stopped because law enforcement monitored it and would show up at people's homes. Burns also stated that he had used TOR³ in the past but didn't like it. When the agents informed him that they were working on a Freenet case, Burns admitted to using Freenet.

CS White explained why the agents were present; specifically, that an individual using Burns's IP address requested child pornography via Freenet. When asked how long he had been using Freenet, Burns stated that he had been using it for a few months. Burns acknowledged that he used Frost⁴ to obtain the information necessary to download files via Freenet. Burns proclaimed that there was no new child pornography on the Internet. He explained that it was all old stuff that he had already seen.

CS White asked Burns what kind of child pornography files he had downloaded. Burns replied that the agents should already know since they were monitoring his downloads. When asked what he did with the child

² Unlike Freenet, anonymity is not a feature of the BitTorrent network.

³ Tor is an online network that obfuscates a user's IP address thereby providing anonymity to online activities. United States v. McLamb, 880 F.3d 685, 688 (4th Cir. 2018). Hidden websites, or "services," are also available through the use of Tor. Id.

⁴ Frost is a software program that works with Freenet to provide newsgroup-like messaging, private encrypted messages, and file upload/download functionality.

pornography files, Burns explained that he downloaded the files to a hard drive and then sorted through them, deleting the files he didn't want. Burns said that he preferred minor girls 15 to 16 years of age. He further specified, the "jailbait" type pictures.

When asked if he had ever taken pictures of a minor female, Burns said that he had never taken a nude picture of a minor girl. When asked if he had ever had sexual contact with a minor, Burns said that he has never done anything like that with a child. Burns also stated that the child pornography was for his personal use and that he did not upload, trade, or sell the images.

Burns denied using any type of encryption software to protect his files. Burns gave CS White verbal consent to take his computer and hard drives and examine them for child pornography. CS White asked Burns which hard drive he used to save the child pornography that he downloaded. In response, Burns explained that there were three hard drives connected to his desktop computer. The first contained the computer's operating system, the second was the location to which files were downloaded, and the third contained music.

During the interview with the agents, Burns sometimes qualified his answers by stating "If I was doing it...." and "...I'm not saying I did it" and then smiling.

Burns executed a written consent permitting CS White to search his devices. With Burns's permission, CS White took custody of the computer and

hard drives. Burns also gave the agents consent to walk through his apartment in order to make sure no other devices were present and no one was hiding. Upon a walk-through, agents didn't observe either. CS White gave Burns his business card and advised him to call if he had any questions.

Forensic Analysis of Electronic Devices:

CS White forensically examined Burns's three computer hard drives. The first was in fact the computer's operating system and contained deleted child pornography files, the second, a 2TB Hitachi with serial number YFGNBBTA, was fully encrypted by VeraCrypt software, and the third did in fact contain music files. SA White's analysis did not reveal any encrypted containers on the first or third drives.

The first hard drive, the operating system, contained 36 child pornography images that CS White recovered from unallocated space (i.e. they had been deleted from the active disk space). In the hard drive's active space, at the file path "user\WSPD Fraud\Desktop," CS White observed instructions on how to setup Freenet and TOR on a full disk encrypted hard drive to prevent data leaks. The instructions were in the form of three images and included how to use VeraCrypt software. CS White also located VeraCrypt software and the TOR browser on the hard drive's active space.

Burns stated that there is also adult pornography on the hard drive. Burns again explained that he liked to download “jailbait” files and preferred girls between 15 and 16 years of age. CS White asked Burns why he was reluctant to provide the password given that Burns had admitted to downloading and possessing child pornography. Burns again stated that it wasn’t in his best interest to enable the agents to see the images stored on his hard drive.

CS White explained that he had already observed child pornography on the Burns’s first hard drive, the operating system. Burns asked, if this was the case, why agents needed access to the encrypted drive. The agents again explained that they wanted to determine whether the minors depicted in the images had been identified and to confirm that Burns’s statement that he had not produced any of the images as he claimed. Burns again stated that it was not in his best interest to provide the password.

Before the agents left, Burns asked them to notify him before they came to arrest him. He said that he would not make it in prison.

Warrant to Search Burns’s Hard Drive:

On October 4, 2018, this Court issued a warrant authorizing the search of Burns’s 2TB Hitachi hard drive. Case No. 1:18mj307. Upon issuance of the warrant, SA Cook sent a forensic copy of the drive to HSI’s Cyber Crime Center (C3). HSI C3 attempted to access the hard drive by means of brute-force decryption. To date, HSI’s efforts have been unsuccessful.

Indictment & Procedural Posture:

On December 17, 2018, a grand jury in the Middle District of North Carolina issued an indictment charging Burns with violations of Title 18 U.S.C. Code §§ 2252A(a)(2)(A), receipt of child pornography, and 2252A(a)(5)(B), possession of child pornography. Case No. 1:18cr492. Burns surrendered himself to law enforcement on December 20, 2018. On December 27, 2018, Burns waived his detention hearing and was ordered detained pending trial. Burns's case, 1:18cr492, is set for change of plea on February 8, 2019.

ARGUMENT & LEGAL AUTHORITY

By this Application under the All Writs Act, the government seeks an order requiring Burns to assist in the effectuation of the search warrant issued on October 4, 2018, by producing the 2TB Hitachi hard drive in a fully unlocked and unencrypted state. An order requiring Burns to produce the hard drive in an unlocked and unencrypted state would not violate his Fifth Amendment privilege against self-incrimination. Accordingly, there is no hindrance to this Court issuing the requested relief.

A. The All Writs Act Empowers This Court to Order the Requested Relief.

The All Writs Act permits federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages

and principles of law.” 28 U.S.C. § 1651(a). It is “a residual source of authority to issue writs that are not otherwise covered by statute.” *Penn. Bureau of Correction v. United States Marshals Serv.*, 474 U.S. 34, 43 (1985). The power conferred by the Act extends to anyone “in a position to frustrate the implementation of a court order or the proper administration of justice,” as long as there are “appropriate circumstances” for doing so. *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977).

Courts have authority under the All Writs Act to issue supplemental orders to facilitate the execution of search warrants. In *New York Telephone*, for example, the district court had issued an order authorizing federal agents to install pen registers in two telephones and directing the New York Telephone Company to furnish “all information, facilities and technical assistance” necessary to accomplish the installation. 434 U.S. at 161. The telephone company moved to vacate the order, arguing that neither Federal Rule of Criminal Procedure 41 nor the All Writs Act “provided any basis” for it. *Id.* at 163. The Supreme Court, however, held that the order was “clearly authorized by the All Writs Act” as a necessary and appropriate means of effectuating the installation of the pen registers. *Id.* at 172.

Under circumstances very similar to this case, the Third Circuit upheld an order under the All Writs Act requiring the defendant to produce unencrypted copies of electronic devices seized from his residence. See *United*

States v. Apple MacPro Computer et al., 851 F.3d 238, 245 (3d Cir. 2017). In *Apple MacPro Computer*, officers had executed a search warrant at the defendant's home, seizing a computer and two encrypted external hard drives. *Id.* at 242. A review of the computer revealed one image of child pornography, evidence that the computer had accessed child pornography websites, and logs showing that child pornography had been transferred to the external hard drives. *Id.* In addition, the defendant's sister told investigators that she had seen child pornography on the external hard drives. *Id.* at 242-43. When the defendant refused to provide the encryption passwords, the government moved for an order under the All Writs Act requiring him to produce the devices in a fully unencrypted state, which the magistrate judge issued. *Id.* at 243. On appeal, the Third Circuit upheld the order under the All Writs Act, holding that it "was a necessary and appropriate means of effectuating the original search warrant." *Id.* at 246. The court reasoned that, as in *New York Telephone*, the defendant was not far removed from the underlying controversy, compliance with the order required minimal effort, and without the defendant's assistance there was no conceivable way in which the search warrant could be effectuated. *Id.*

Just last year, again in circumstances very similar to this case, a judge in the Northern District of California reached the same conclusion. See *United States v. Spencer*, 2018 WL 1964588 (N.D. Cal. 2018). In *Spencer*, agents had

executed a search warrant at a residence. *Id.* at *1. They seized multiple devices, some of which contained child pornography and some of which were encrypted. *Id.* Significant evidence existed that the defendant owned the encrypted devices, knew the passwords, and that the devices contained child pornography. *See Id.; In re Search of a Residence in Aptos, Calif.* 95003, 2018 WL 1400401 at *1-*4 (N.D. Cal. 2018). Upon motion by the government, a magistrate judge issued an order under the All Writs Act directing the defendant to decrypt the devices. *Spencer* at *1. *Citing Apple MacPro Computer*, the District Court found that reliance on the All Writs Act to issue the order was appropriate. *Id.* at *4.

Other courts have also issued orders under the All Writs Act compelling assistance with circumventing password protections or decryption where the device at issue was the subject of a valid search warrant. *See, e.g., United States v. Blake*, 868 F.3d 960, 971 (11th Cir. 2017) (holding that the district court had the power under the All Writs Act to order Apple Inc. to assist the FBI in bypassing an iPad's passcode and other security measures and noting that "there was no other way for the FBI to execute the district court's order to search the contents of the iPad" as commanded by the search warrant); *In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant*, 2014 WL 5510865 at *2-*3 (S.D.N.Y. 2014) (citing the All Writs Act and requiring manufacturer to provide assistance in unlocking cell phone unless

compliance would be unreasonably burdensome); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1238 (D. Colo. 2012) (granting application under the All Writs Act to require the owner of a computer seized pursuant to a search warrant to produce it in an unencrypted state).

In accordance with these principles, this Court should issue an order under the All Writs Act requiring Burns to assist with the execution of the search warrant issued on October 4, 2018, by producing the 2TB Hitachi hard drive in a fully unlocked and unencrypted state. Without his assistance, the search warrant will be frustrated, because the government will be unable to search the hard drive for the information specified in the warrant. Burns is not far removed from the underlying controversy, and the requested relief will not impose an unreasonable burden on him; he need only enter the necessary password. Moreover, with the proliferation of encryption technology, the government would be significantly hampered in its ability to prosecute crimes if the Court could not require a defendant to unencrypt devices lawfully seized for search.

B. The Requested Relief Would Not Violate Burns's Fifth Amendment Privilege Against Self-Incrimination.

The government anticipates that Burns will argue that an order requiring him to produce the 2TB Hitachi hard drive in an unencrypted state violates his Fifth Amendment right against self-incrimination. The

government will therefore explain why such an order would not implicate Burns's Fifth Amendment privilege.

1. The Contents Of The Hard Drive Are Not Privileged, Because Burns Was Not Compelled To Create Or Store Them.

The Fifth Amendment states that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself.” U.S. Const. Am. V. However, the Fifth Amendment “does not independently proscribe the compelled production of every sort of incriminating evidence”; it applies “only when the accused is compelled to make a Testimonial Communication that is incriminating.” *Fisher v. United States*, 425 U.S. 391, 408 (1976). Put another way, to implicate the Fifth Amendment privilege, a defendant must show a (1) compelled (2) testimonial communication or act (3) that is incriminating. *Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty.*, 542 U.S. 177, 189 (2004).

As an initial matter, the 2TB Hitachi hard drive’s contents are not privileged, because they were not created or stored under compulsion. See *Fisher*, 425 U.S. at 409-10 (holding that, where certain tax-related papers sought by the government had been voluntarily prepared, they “[could not] be said to contain compelled testimonial evidence” and therefore were not privileged); see also *United States v. Doe*, 465 U.S. 605, 611-12 (1984) (holding that the contents of documents were not privileged where respondent “[did] not contend that he prepared the documents involuntarily or that the subpoena

would force him to restate, repeat, or affirm the truth of their contents"). The mere fact that the devices' contents may be incriminating—and, depending on the nature of the files, possibly testimonial—is insufficient to implicate the privilege. *See Fisher*, 425 U.S. at 409-10 (concluding that a subpoenaed taxpayer could not "avoid compliance with the subpoena merely by asserting that the item of evidence which he is required to produce contains incriminating writing, whether his own or that of someone else"). Because the government did not compel Burns to create, obtain, or store any information on the hard drive, its contents are not protected by the Fifth Amendment.

2. The Act Of Producing The 2TB Hard Drive In An Unencrypted And Unlocked State Is Not Privileged, Because The Foregone Conclusion Doctrine Applies.

Because the information on the hard drive is not privileged, the only question is whether the very act of producing the hard drive in an unencrypted and unlocked state implicates the Fifth Amendment. The answer is no.

The Fifth Amendment does not proscribe the compelled production of evidence if the facts communicated by the act are foregone conclusions. *Fisher v. United States*, 425 U.S. 391 (1976), provides the framework for applying the Fifth Amendment privilege to the compelled production of evidence. In that case, the government had issued summonses for several categories of documents related to an individual's tax returns. 425 U.S. at 394-95. In concluding that enforcement of the summonses did not violate the Fifth

Amendment, the Court distinguished between two types of communications inherent in the production of the records.

On the one hand, the Court held that the contents of the records were not privileged because the documents had been prepared voluntarily prior to the issuance of the summonses and were therefore not the taxpayer's compelled testimony. *Fisher*, 425 U.S. at 409-10.

On the other hand, the Court recognized that the act of production itself could communicate potentially incriminating facts, including, a tacit concession that the papers existed, that the respondent possessed them, and that they were authentic. *Fisher*, 425 U.S. at 410. Nevertheless, the Court held that the compelled act of producing the papers did not implicate the Fifth Amendment because “[t]he existence and location of the papers [were] a foregone conclusion and the taxpayer add[ed] little or nothing to the sum total of the Government’s information by conceding that he in fact ha[d] the papers.” *Id.* at 411.

Put another way, because the potentially testimonial aspects of the act of production were a “foregone conclusion,” compliance with the summonses became a question “not of testimony but of surrender.” *Id.* (quoting *In re Harris*, 221 U.S. 274, 279 (1911)). *See also United States v. Hubbell*, 530 U.S. 27, 45 (2000) (holding that the “foregone conclusion” doctrine espoused in *Fisher* did not apply where “the Government has not shown that it had any

prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent"); *United States v. Stone*, 976 F.2d 909, 911 (4th Cir. 1992) (finding no Fifth Amendment violation of compelled production when documents' "existence, possession, and authentication are a 'foregone conclusion'").

The act of producing an electronic device in an unencrypted state has potentially testimonial components similar, but not identical, to the potentially testimonial components involved in the act of responding to a subpoena for particular categories of documents. First, producing documents in response to a category-based subpoena demonstrates the document's existence; producing an unencrypted device will similarly demonstrate the device's existence. Second, compliance with a category-based subpoena demonstrates possession and control over the documents; producing an unencrypted device will similarly demonstrate possession and control over the device.

Regarding the knowledge implicitly demonstrated by the act of production, however, producing specified unencrypted devices may differ from producing specified categories of documents in response to a subpoena. Producing papers in response to a category-based subpoena implicitly demonstrates knowledge of the contents of the papers produced: It demonstrates the "belief that the papers are those described in the subpoena." *Fisher*, 425 U.S. at 410. In contrast, producing a device in an unencrypted state

implicitly demonstrates knowledge of the encryption password for the device, but it does not necessarily imply knowledge of the device's contents, because such knowledge is not needed to produce the device in an unencrypted state.⁵ Nevertheless, the government recognizes that where, as here, a search warrant has been issued for an individual's device based on probable cause to believe that it contains child pornography, the individual's ability to produce the device in an unencrypted state will generally provide strong evidence of the individual's knowledge of its contents. Accordingly, the government proceeds on the assumption that the production here of the unencrypted electronic devices includes the potentially testimonial aspects of the act of production in *Fisher*—namely, that the targeted hard drive exists and belongs to Burns, that the Burns can decrypt the hard drive, and that the hard drive contains child pornography.

Several courts have held that the foregone conclusion doctrine applies where the government can show independent knowledge of the facts communicated by the act of producing an electronic device in a decrypted state. In *Apple MacPro Computer*, for example, where the defendant had shown his sister child pornography stored on his external hard drive, the government

⁵ For example, Jane might know the four-digit passcode to her friend's iPhone from observing the friend enter the passcode on many occasions. Jane could unlock the iPhone by entering the passcode even though she has no knowledge of the phone's contents.

provided evidence both that child pornography “files exist[ed] on the encrypted portions” of the hard drive and that the defendant “[could] access them.” 851 F.3d at 248. Accordingly, the Third Circuit held that it was not plain error for the magistrate judge to conclude that “any testimonial component of the production of [the] decrypted devices added little or nothing to the information already obtained by the Government” and was therefore a foregone conclusion. *Id.* The Third Circuit thus rejected the defendant’s Fifth Amendment challenge to an order requiring him to produce his hard drive in a decrypted state.⁶

The district court in *In re Boucher*, 2009 WL 424718 (D. Vt. 2009), reached the same conclusion under similar circumstances. In that case, an agent at a border crossing observed that Boucher’s computer contained child pornography and Boucher explained that he sometimes accidentally downloaded such material. *Id.* at *1-2. The agent seized the computer and obtained a search warrant, but he was later unable to access the child pornography because the drive was encrypted. *Id.* at *2. Reasoning that the government had shown independent knowledge of “the existence and location of the [relevant] drive

⁶ In *Apple MacPro Computer*, the Third Circuit noted that “a very sound argument can be made” that the foregone conclusion doctrine in the decryption context properly focuses on whether the Government already knows that a defendant can decrypt a device, and that the government need not demonstrate knowledge of the device’s contents. 851 F.3d at 248 n.7. As noted previously, however, the government proceeds in this matter on the assumption that it must also demonstrate its knowledge that the targeted devices contain child pornography.

and its files,” the court applied the foregone conclusion doctrine and ordered Boucher to produce the computer in an unencrypted state. *Id.* at *3-4. *See also United States v. Spencer*, 2018 WL 1964588 (N.D. Cal. 2018) (applying foregone conclusion doctrine and compelling assistance with decryption); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 614 (Mass. 2014) (same); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012) (same).

In contrast, where officers lacked evidence either that a defendant knew the password for encrypted devices or that there were any child pornography files stored on them, the Eleventh Circuit held that the government had failed to make the factual showing necessary to invoke the foregone conclusion doctrine. *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012). In that case, law enforcement officers conducting a child pornography investigation seized encrypted electronic storage media from the defendant’s hotel room, but they lacked specific evidence that the defendant could decrypt them or that they stored child pornography. *See id.* at 1338-39, 1346. Under these circumstances, the court concluded that the foregone conclusion doctrine did not apply because the government had failed to show “that encrypted files exist on the drives, that [the defendant] has access to those files, or that he is capable of decrypting the files.” *Id.* at 1349.

Here, the government can satisfy even the exacting standards set by the Eleventh Circuit for the application of the foregone conclusion doctrine. The government can demonstrate that Burns owned and controlled the hard drive at the time of its seizure, that he can decrypt it, and that it contains child pornography files. Under the foregone conclusion doctrine, Burns's act of producing the decrypted device is not protected by the Fifth Amendment.

First, the government can establish that the hard drive exists and belongs to Burns. Investigators recovered the hard drive from Burns's residence, of which he is the sole occupant. Burns identified the hard drive as his and described how he used it: to store downloaded content.

Second, the government can establish that Burns knows the password and can decrypt the device. Burns lived alone and stated that he used the device to store encrypted child pornography, which alone would imply his ability to decrypt it. But there is more: he stated that he preferred not to provide the password because letting the agents see the files would not be in his best interest, thereby directly indicating that he in fact knows the password.

Third and finally, the government can establish that there are child pornography files on the hard drive. Burns admitted that he uses the drive to store child pornography. This admission is corroborated by the fact that CS White identified Burns as an individual who was likely downloading child

pornography via the Freenet peer-to-peer network and subsequently recovered child pornography from Burns's operating system hard drive.

CONCLUSION

The government seeks an order under the All Writs Act, Title 28 U.S.C. § 1651 compelling the defendant to produce his hard drive in an unlocked and decrypted state. This can be accomplished by ordering Burns to enter the password without revealing it to law enforcement. The contents of the hard drive are not privileged and Burns's act of production would not be testimonial, since the only potentially testimonial components implicit in his act of producing the unlocked/unencrypted hard drive are foregone conclusions.

This the 6th day of February, 2019.

Respectfully submitted,

MATTHEW G.T. MARTIN
UNITED STATES ATTORNEY



ERIC L. IVERSON
Assistant United States Attorney
NCSB #46703
United States Attorney's Office
Middle District of North Carolina
101 S. Edgeworth St., 4th Flr.
Greensboro, NC 27401
Phone: 336/332-6302